Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 11, Issue 1 (January-June) 2026
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

Audit Procedure for Selecting Providers through E-Procurement (LPSE)

✉A,B,C,D,E,FBobby Yuhanda, FRatna, FAbdullah, B,C,FFaiz Muttaqin Simbolon
Inspektorat Aceh, Indonesia

ARTICLE INFORMATION
Article History:
Received July 18, 2025
Revised April 8, 2026
Accepted June 8, 2026

DOI:
10.21532/apfjournal.v11i1.419

A – Research concept and design
B – Collection and/or assembly of data
C – Data analysis and interpretation
D – Writing the article
E – Critical revision of the article
F – Final approval of article

ABSTRACT
This study examines the effectiveness of e-audit implementation in the e-procurement (LPSE) system, focusing on fraud risks in the supplier selection process. Using a qualitative case study approach, the research analyzes 2023 procurement data, including access logs, document metadata, and system-generated reports. The findings reveal significant vulnerabilities, such as unauthorized user ID usage, inconsistencies in activity logs, weak access controls, similarities in IP addresses, and identical document metadata among bidders, indicating potential collusion and manipulation. These weaknesses suggest that current e-audit practices are not fully integrated and remain partially manual, limiting their effectiveness in detecting fraud. Drawing on internal control and fraud theories, this study highlights gaps between regulatory compliance and operational implementation. The study proposes a technology-driven e-audit framework, including multi-factor authentication, automated audit modules, and digital forensic analysis. Strengthening these aspects is essential to enhance transparency, accountability, and integrity in electronic procurement systems.

Keywords: *E-Audit, E-Procurement, LPSE, Fraud Detection, Digital Forensics, Collusion.*

How to Cite:
Yuhanda, B., Ratna, Abdullah, & Simbolon, F. M. (2026). Audit Procedure for Selecting Providers through E-Procurement (LPSE). *Asia Pacific Fraud Journal, 11*(1), 169-187. https://doi.org/10.21532/apfjournal.v11i1.419.

✉Corresponding author :
Email: bobbyyuhanda@ymail.com

1. INTRODUCTION

The implementation of electronic procurement (e-procurement) systems has been widely adopted to enhance transparency, efficiency, and accountability in public procurement processes. However, public procurement remains vulnerable to fraud and corruption due to process complexity and multi-stakeholder involvement (OECD, 2016; Klitgaard, 1998). In Indonesia, e-procurement is managed through the LPSE system under LKPP regulations.

Despite established regulatory frameworks (LKPP, 2022; Kementerian Keuangan RI, 2020), fraud risks persist, including unauthorized access and collusion (Liu et al., 2020; Zhang & Zhao, 2021). Weak internal controls and limited analytical integration contribute to these vulnerabilities (COSO, 2013; Singleton & Singleton, 2010).

The transformation from conventional to electronic systems introduces new risks, including weak audit trails, access control vulnerabilities, and increased system complexity requiring advanced technical competencies. Prior studies predominantly emphasize procedural compliance and performance outcomes, with limited focus on forensic-based detection of fraud within digital procurement environments.

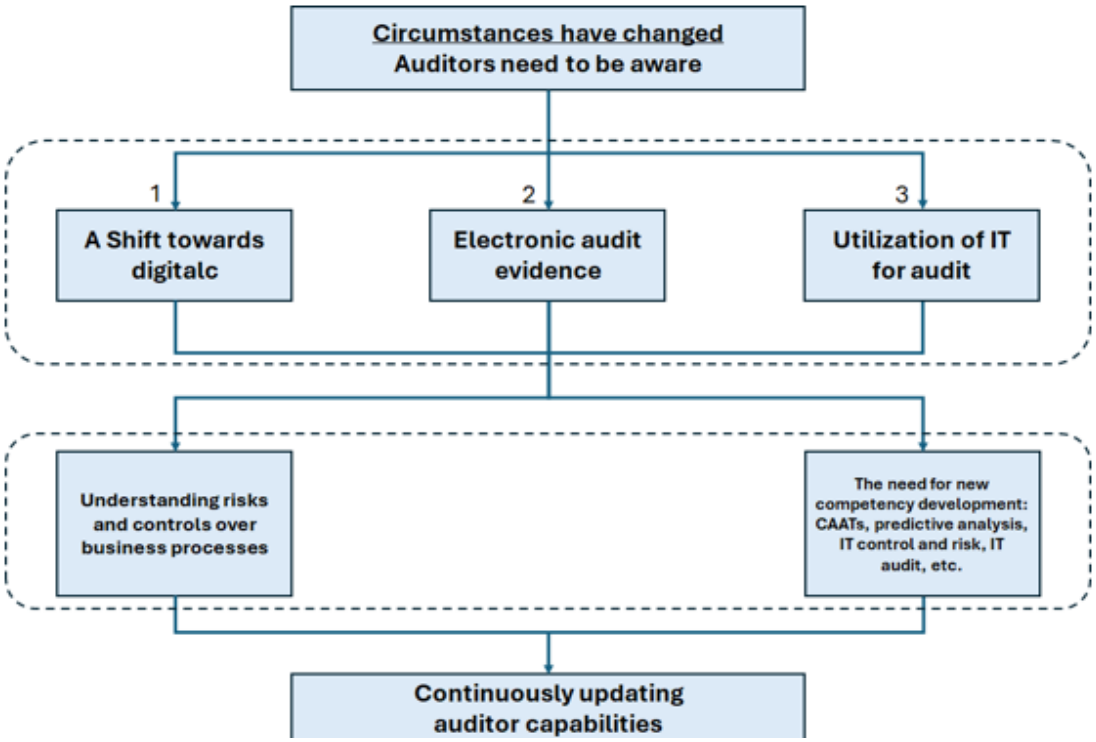
Figure This figure illustrates how changes in the business environment and technology influence audit practices and the competencies required of auditors. Key changes (top section) :

a. A shift towards digital, The transition to digital systems in business processes.
b. Electronic audit evidence, Audit evidence is now largely in electronic form.
c. Utilization of IT for audit, The use of information technology in audit processes.

These three factors indicate that auditing is no longer conventional but has become technology-based. Implications for auditors (middle section): Auditors must understand risks and controls in increasingly complex, system-based business processes. They also need to develop new competencies, such as :

a. CAATs (Computer-Assisted Audit Techniques)

Figure 1. **Circumstances Have Changed: Auditors Need to Be Aware**



b. Predictive analytics
c. IT audit and IT risk control

Main conclusion (bottom section): Auditors are required to continuously update their capabilities (continuous improvement) to remain relevant in line with technological advancements and emerging risks. In addition to reducing and even eliminating many risks in manual systems, the implementation of information technology can also introduce new risks specific to digital systems. Ignoring these risks can lead to significant losses, such as data loss, reliance on inaccurate information, or material misstatements in financial statements. Specific risks in information technology systems include:

a. Risks to Hardware and Data Security
   Hardware damage or failure can result in the loss of critical data. Meanwhile, weaknesses in security systems can open the door to unauthorized access, data theft, or cyberattacks that threaten the integrity of information.
b. Reduced Audit Trail in Electronic Processes
   Electronic systems can reduce transparency if they are not designed with adequate record-keeping mechanisms. Without complete and verifiable activity logs, auditors will have difficulty tracking data changes, identifying suspicious activities, and ensuring accountability at every stage of the process.
c. The Increasing Need for Specialized Skills in the Field of Information Technology (IT)
   With the complexity of digital systems, organizations need human resources with a deep understanding of information technology. A lack of expertise in this area can hinder effective system management, increase the risk of operational errors, and reduce the ability to detect and address cybersecurity threats.
d. Challenges in Segregation of Duties and Access Control in Information Technology Systems
   In manual systems, segregation of duties can be more easily achieved through organizational structures and internal policies. However, in electronic systems, inadequate access management can lead to conflicts of interest, where an individual has excessive access rights, allowing data manipulation to occur without detection. Therefore, implementing Role-Based Access Control (RBAC) is crucial to ensure that each user only has access rights commensurate with his or her responsibilities.

These risks must be managed and addressed carefully and systematically to ensure the integrity, security, and reliability of electronic systems to support effective and transparent operations. Some approaches that can be implemented include:

a. Implementation of IT Risk Management: Identifying, analyzing, and mitigating potential threats to electronic systems through security policies, regular monitoring, and rapid response to incidents.
b. Strengthening Data and Infrastructure Security: using encryption, firewalls, and intrusion detection systems to protect data and prevent unauthorized access.
c. Improved Audit Trail and Transparency: developing a system that records all user activity to increase accountability and simplify the audit process.
d. Human Resources Training and Skills Development: ensuring that human resources have an adequate understanding of cybersecurity, data processing, and electronic system management.
e. Implementation of Strict Access Control: Implementing mechanisms such as Role-Based Access Control (RBAC) to restrict access based on user responsibilities and reduce the risk of data manipulation.

By implementing these steps, organizations can reduce the negative impact of information technology risks and

ensure that electronic systems remain secure and reliable and support the principles of transparency and accountability. Environmental changes and the increasing use of information technology have made it a key enabler in government, supporting business process efficiency and improving the quality of public services. However, information technology also brings new risks that require specific controls tailored to the characteristics of electronic systems. Therefore, auditors must adapt their methods of collecting and analyzing audit evidence by shifting to an electronic data-based approach. The objectives are:

a. Improving accuracy and efficiency in detecting anomalies or indications of non-conformity in the system.
b. Ensuring transparency and accountability in government processes through more digital evidence-based audits.
c. Leveraging technologies such as data analytics, forensic audit tools, and machine learning to identify suspicious patterns or hidden potential risks.

By taking these approaches, auditors can be more effective in maintaining the integrity of electronic government systems, ensuring that the use of information technology not only increases efficiency, but also remains within the corridor of good governance. In response to this condition, this study raises this problem as a case study with the title: "*Audit Procedure for Selecting Providers through E-Procurement (LPSE)*."

This study aims to analyze vulnerabilities in the LPSE system and develop a structured e-audit approach to enhance fraud detection and procurement integrity. Research Gap and Contribution. This study addresses the gap by integrating digital forensic techniques (log correlation, metadata analysis, hash verification, and IP tracing) into e-procurement audit procedures. It proposes a forensic-based e-audit framework that enables systematic detection of technologically enabled fraud schemes. The study contributes theoretically by linking fraud theory with digital audit evidence, and practically by offering implementable controls and analytics for LPSE. Research Objective. To identify fraud risk indicators and control weaknesses in LPSE and to develop a forensic-oriented audit approach that enhances detection and prevention capabilities.

2. LITERATURE REVIEW AND HYPOTHESIS

Fraud in Public Procurement

Public procurement is inherently vulnerable to fraud due to high transaction values, complexity of processes, information asymmetry, and the involvement of multiple actors. The Fraud Triangle theory (pressure, opportunity, and rationalization) provides a fundamental framework to explain fraud occurrence. In digital procurement environments, the "opportunity" dimension becomes more dominant, particularly when internal controls such as access control, audit trails, and system monitoring are weak or improperly implemented. These conditions increase the likelihood of unauthorized access, manipulation, and collusive behavior.

E-Procurement and Fraud Risk

While e-procurement systems are designed to enhance transparency and accountability, prior studies indicate that they also introduce new forms of risk. These include unauthorized system access, data manipulation, off-system transactions, and potential system-level intervention. In many cases, formal compliance with regulations does not guarantee effective fraud prevention, especially when audit mechanisms remain conventional and are not integrated with real-time system analytics. Consequently, vulnerabilities within digital platforms can be exploited to facilitate non-transparent practices.

Digital Forensic Audit

Digital forensic auditing has emerged as a critical approach for detecting fraud in

information systems. It utilizes electronic evidence such as access logs, document metadata, hash values, and network traces to identify anomalies and reconstruct system activities. Compared to traditional audit methods, forensic-based approaches provide higher evidential reliability and enable more precise detection of irregularities, including unauthorized access, data manipulation, and coordinated behavior among system users.

Conceptual Framework and Hypothesis Development

Based on the theoretical foundations and prior empirical findings, this study proposes an integrated conceptual framework linking fraud drivers, control weaknesses, and forensic detection mechanisms. The framework consists of:

a. Fraud drivers (pressure, opportunity, rationalization)
b. Control weaknesses (weak role-based access control, inadequate logging, and non-integrated audit systems)
c. Digital evidence (logs, metadata, hash values, and IP addresses)
d. Forensic analytics (correlation, validation, and pattern detection)
e. Fraud indicators (anomalies, collusion signals, and manipulation patterns).

This framework underpins the development of the study hypotheses, which posit that weaknesses in access control, inconsistencies in system logs, similarities in digital evidence, and patterns in network activity are significantly associated with fraud risks in e-procurement systems. By integrating forensic analytics into the audit process, this study aims to enhance the detection of irregularities and strengthen the integrity, transparency, and accountability of electronic procurement systems.

This study employs an exploratory case study design with a qualitative approach to examine fraud risk indicators and control weaknesses in an electronic procurement (e-procurement) system. The case focuses on the LPSE platform implemented within a government agency, selected to enable an in-depth assessment of system vulnerabilities and potential irregularities in the procurement process.

Data were derived from primary procurement records and system-generated information, including bid documents and transaction summaries. The analysis was conducted using a descriptive and evidence-based approach, integrating elements of digital forensic analysis to identify patterns indicative of potential misconduct. Specifically, the study examines document metadata, system access logs, and file hash values to detect inconsistencies and possible data manipulation. In addition, Internet Protocol (IP) address analysis was performed to identify similarities among participants that may suggest coordinated behavior or unauthorized collaboration. This methodological approach enables a systematic identification of anomalies and strengthens the reliability of findings related to fraud risk detection in digital procurement environments.

a. Data Collection

This study relies on primary data obtained from electronic procurement report summaries, access logs, and document properties/metadata, which serve as the empirical basis for the analysis. Data are collected through direct access to the e-procurement (LPSE) system and documentation related to the electronic tendering process to ensure the accuracy, relevance, and validity of the information analyzed. This approach allows for the identification of potential weaknesses in the system, including indications of data manipulation, unauthorized access, and practices that undermine the transparency and integrity of electronic procurement.

b. Tender Approval Procedure Analysis

This stage includes an in-depth analysis of the user identities used in the tender approval process, comparing them to the committee structure within the Procurement Services Unit (ULP) and the Procurement Service Unit Working

Group (Pokja ULP). Every activity related to the access data from each user identity is examined in detail to identify potential manipulation, abuse of authority, or unauthorized use. This analysis aims to ensure that every transaction in the system complies with established authorizations, detect any irregularities that can threaten the transparency and integrity of the electronic procurement process, and validate the timing of user identity use. Every activity recorded in the e-procurement (LPSE) application access log is analyzed to ensure that the user's identity is active within the timeframe consistent with his or her authorization. User activity, from registration to filing complaints, is thoroughly reviewed to detect any unauthorized actions, discrepancies, or anomalies in access usage.

c. Access Control Check

This study evaluates the level of understanding of the e-procurement (LPSE) system among the Procurement Service Unit/Working Group (ULP/ Pokja) members and identifies any processes that may have been delegated to external parties. Every user identity activity with specific access rights is thoroughly verified to ensure that all actions are carried out in accordance with the assigned tasks and authorities. Furthermore, an in-depth analysis is conducted to detect inconsistencies in access usage and potential misuse of access rights that can threaten the transparency, security, and integrity of the electronic procurement system.

d. Collusion Test

Potential collusion between the Procurement Service Unit/Working Group (ULP/Pokja) members and auction participants is analyzed by examining the hash values of encrypted files using the Apendo document security application. These hash values are verified against e-procurement (LPSE) system records to identify discrepancies that can indicate unauthorized document manipulation or modification. This analysis aims to maintain data integrity, ensure transparency, and prevent fraudulent practices in the e-procurement process.

e. Bidding Document Properties Analysis/Metadata Files

Metadata from the bidding documents, including the creation and modification dates, and the identity of the bidder, is analyzed to ensure they are authentic and have not been altered during the bidding process. This metadata is then compared with records in the e-procurement (LPSE) system to verify the validity of the documents and detect potential modification or manipulation by unauthorized parties. This analysis plays a critical role in maintaining integrity and transparency in the e-procurement process.

f. Detection of Collaboration between Participants

This study analyzes each participant's IP address to detect potential similarities that can indicate collaboration or unauthorized collusion. The analysis is comprehensive, covering all stages of the tender, from registration to filing objections, to ensure that suspicious interaction patterns can be accurately detected. Furthermore, participant access patterns and activity times are examined to identify potential unnatural coordination, which can potentially undermine the integrity and transparency of the electronic auction process.

g. E-Procurement (LPSE) Application Availability Testing

A forensic audit of the e-procurement (LPSE) server is conducted to assess network capacity and identify potential deliberate access restrictions during the tender period. An in-depth analysis of server logs is conducted to detect any indication of manipulation of system availability settings that can potentially benefit certain parties. Furthermore, a thorough evaluation of disruption patterns, access anomalies, and system

performance degradation is conducted to ensure that no interventions are detrimental to transparency and fairness in the e-procurement process.

h. Data Analysis and Interpretation of Findings

The results of each test are analyzed descriptively to identify patterns and trends that reveal weaknesses in the security and integrity of the e-procurement process. These findings are examined in depth to understand the factors contributing to potential risks and gaps in the system. Based on the analysis, strategic recommendations are developed to strengthen the reliability, increase transparency, and optimize the effectiveness of the e-tender system. These steps are expected to minimize opportunities for manipulation and ensure a more accountable and equitable procurement process.

3. METHODS

This study employs a qualitative case study approach to analyze the implementation of e-audit procedures in the e-procurement (LPSE) system. The focus is on identifying fraud risks and control weaknesses in the supplier selection process.

The data consist of procurement data from 2023, including access logs, document metadata, and system-generated reports. These data are considered reliable digital audit evidence as they provide traceable records of system activities (Singleton & Singleton, 2010; Zhang & Zhao, 2021).

Data collection was conducted through documentation techniques by extracting electronic records from the LPSE system in accordance with applicable regulations governing electronic procurement (LKPP, 2022). The study applies a data-driven audit approach using digital forensic techniques, including log analysis, metadata examination, and hash verification, to ensure data integrity and audit reliability (Vasarhelyi et al., 2015).

The analysis was conducted through several stages. First, testing of e-tender approval procedures was performed by examining summary reports to verify authorization and compliance with internal control principles (COSO, 2013; Arens et al., 2020). Second, the validity of user ID usage was analyzed through access logs to detect anomalies and unauthorized access (ACFE, 2022).

Third, access control testing was conducted by reviewing user activities of the Procurement Service Unit (ULP) Working Groups to ensure that all actions were performed by authorized personnel, as weak access control is a critical risk in information systems (Behl & Behl, 2017). Fourth, testing for potential collusion was carried out through hash value verification and log analysis to identify possible manipulation of bidding documents (Zhang & Zhao, 2021).

Fifth, metadata analysis was performed to examine file properties and detect similarities among bidding documents, which may indicate coordinated behavior among participants (Liu et al., 2020). Sixth, IP address analysis was conducted to identify patterns of shared system access, which may suggest collusion or bid rigging practices (OECD, 2016).

Finally, system availability analysis was conducted to detect potential manipulation of system performance during critical stages of the tender process. Data validation was ensured through triangulation of multiple data sources and adherence to government internal audit standards (SAIPI) (Kementerian Keuangan Republik Indonesia, 2020; BPKP, 2021).

The study applies a structured e-audit framework focusing on digital evidence analysis. Key audit procedures include:

Verification of E-Tender Approval through Summary Reports and User ID Validation

This procedure evaluates the validity of tender approval by analyzing summary reports as primary audit evidence. The user ID used for approval is verified against the authorized committee structure. Discrepancies between authorized roles and actual system access are further

examined through access log validation to detect potential misuse or unauthorized approval activities.

The summary report is the foundation of e-procurement (LPSE) oversight, integrating monitoring, auditing, and integrity enforcement. This document serves as key evidence for verifying tender approval procedures because it records all procurement activities. Without it, detecting anomalies and collusion would be difficult. In e-tender approval testing, the summary report serves as the basis for verifying authorization and regulatory compliance.

The initial stage of the e-tender process begins when the Procurement Service Unit (ULP) and the ULP Working Group (Pokja ULP) gain access to the e-tender system through user IDs managed by the e-procurement (LPSE). Each member has limited access rights according to their role, while the authority to approve tenders is officially granted only to the Head of the Working Group as part of an internal control mechanism. This access structure is designed to maintain process integrity, prevent abuse of authority, and increase transparency and accountability. However, cases of tender approvals using user IDs other than those of the Working Group Head have been identified, in violation of the established structure. This indicates the potential for access manipulation outside the official e-procurement (LPSE) system, which not only threatens the integrity of the e-tender process but also opens up opportunities for non-transparent practices and weakens the effectiveness of oversight.

To identify this issue, auditors analyze the summary report to verify the user ID used in the e-tender approval and compare it to the registered committee structure. Furthermore, the auditors request that the relevant user provide a screenshot of the access log data, including the time and date of the e-tender approval. This step aims to ensure the integrity of the approval process and detect any potential misuse or manipulation of access within the e-procurement (LPSE) system.

Figure 2. **Summary Report**

SUMMARY REPORT

Informasi Tender	
Kode Tender	49293106
Nama Tender	Pembangunan Bangunan Perkuatan Tebing Sungai Krueng Teunom Kab. Aceh Jaya
K/L/P/D	Pemerintah Daerah Provinsi Aceh
Satuan Kerja	DINAS PENGAIRAN ACEH
Jenis Pengadaan	Pekerjaan Konstruksi
Metode Pengadaan	Pascakualifikasi Satu File - Harga Terendah Sistem Gugur
Anggaran	Tahun: 2023 / Sumber Dana: APBD / Nilai: Rp. 12.135.686.924,00
Nilai Pagu	Rp. 12.135.686.924,00
Nilai HPS	Rp. 12.135.680.000,00
Jenis Kontrak	Harga Satuan
Kualifikasi Usaha	Kecil
Lokasi Pekerjaan	Krueng Teunom Kab. Aceh Jaya - Aceh Jaya (Kab.)
Persyaratan Kualifikasi	**Persyaratan Kualifikasi Administrasi/Legalitas** **Izin Usaha** Izin Usaha — Sesuai dokumen pemilihan dan masih berlaku 1. Peserta yang melakukan Kerja Sama Operasi (KSO) maka jumlah anggota KSO dapat dilakukan dengan batasan paling banyak 3 (tiga) perusahaan dalam 1 (satu) kerjasama operasi 2. Peserta yang berbadan usaha harus memiliki Surat Ijin Usaha Jasa Konstruksi (IUJK) 3. Memiliki Sertifikat Badan Usaha (SBU) dengan Kualifikasi Usaha Kecil [Kecil/Menengah/Besar], serta disyaratkan sub bidang klasifikasi /layanan Sesuai dokumen pemilihan [sesuai dengan sub bidang klasifikasi/layanan SBU yang dibutuhkan] 6. Memiliki NPWP dan telah memenuhi kewajiban pelaporan perpajakan (SPT Tahunan) tahun pajak 2022 [tuliskan tahun pajak

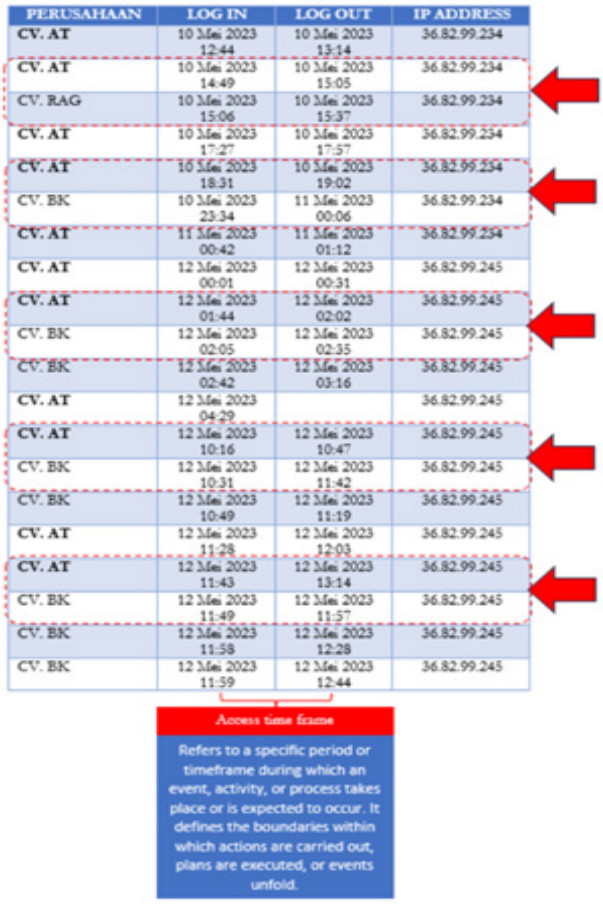
Analysis of user ID Activity Periods Using Access Logs

Access log data are analyzed to assess the consistency between recorded user activities and the predefined e-tender timeline. The analysis focuses on identifying missing logs, abnormal access duration, or activities conducted outside the permitted timeframe, which may indicate the use of unauthorized accounts or off-system processes.

Auditors discover user IDs are not recorded in the activity log at crucial stages, indicating the use of unauthorized accounts or processes outside the e-procurement (LPSE) system with potential manipulation that can threaten procurement integrity. Participant access logs serve as audit evidence, recording all activities (registration, document downloads, bid uploads, and communications) and the duration of user ID usage. The duration of user ID usage serves to maintain transparency and accountability in tenders and detect violations.

Figure 3 illustrates the anomalous timeframe for using user IDs while following a fixed schedule for each stage, from the announcement to the determination of the winner, with a clear time limit to ensure order, transparency and accountability. The auditors conduct further verification by analyzing access log data from e-tender participant user IDs, from the registration stage to the submission of objections. This data is cross-checked with a special identification icon next to the participant's name to ensure that all recorded activities correspond to the login time in the system. This step aims to ensure that every transaction and interaction in the system is accurately documented, carried out within the specified timeframe, and is free from potential manipulation. Thus, the accuracy and legitimacy of the entire e-tender process can be optimally maintained.

Figure 3. **Validation of User ID Usage Period**



Evaluation of Access Control within the ULP Working Group

This stage examines the integrity of user access within the Procurement Service Unit (ULP) Working Group. User activity logs are reviewed to identify anomalies or irregular patterns. Verification is conducted through cross-checking system records and direct confirmation with the respective users to ensure accountability and prevent unauthorized access or delegation.

The auditors review the user ID activity of each Procurement Service Unit (ULP) Working Group by examining summary reports and analyzing log data to detect any anomalies or access abuse. Next, direct clarification is conducted with the user ID owner to ensure that every recorded activity is actually carried out by the individual concerned. If any discrepancies are found, the auditors will investigate the possibility of an unauthorized user ID or external intervention. This process aims to uphold the operational validity of the e-procurement (LPSE) system, maintain the integrity and accuracy of recorded data, and strengthen the access control system to prevent the risk of manipulation or information leakage.

Detection of Potential Collusion through Hash Value Comparison and Encrypted Document Analysis

Bid document integrity is tested through hash value comparison between submitted files and system records. Hash verification is performed using tools such as MD5summer to detect any unauthorized modification. In addition, access logs and file metadata are analyzed to identify premature access or distribution of encrypted documents, which may indicate collusion.

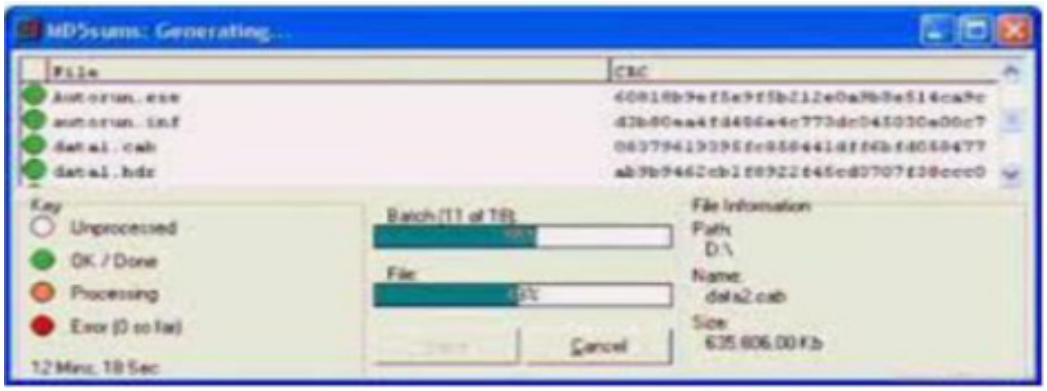
In addition, auditors review access logs to detect any indication that the Procurement Service Unit (ULP) Working Group opens or distributes documents before the specified time. File metadata is also examined to ensure that documents are not modified after the initial upload process. This analysis aims to maintain the confidentiality and integrity of bid documents and prevent potential data leaks or manipulation that could compromise the transparency of the auction process.

If discrepancies in hash values or suspicious access to encrypted files are found, this could be a strong indication of collusion between the Procurement Service Unit (ULP) Working Group and e-tender participants. These findings serve as the basis for formulating recommendations for improvements in monitoring access to tender documents to ensure transparency, accountability, and fairness throughout the e-tender process.

To detect potential collusion between the Procurement Service Unit (ULP) Working Group and the Provider, the auditors test the hash values of encrypted files obtained from the Procurement Service Unit (ULP) Working Group's computer, one of which is by using the MD5summer application. The auditors verify the hash values of the files and compare them with the hash values recorded in the e-procurement (LPSE) system. If there is a difference in the hash values, this indicates that the file being analyzed is not identical to the original file uploaded by the participant. This difference may indicate modification or manipulation outside the e-procurement (LPSE) system. This test plays an important role in identifying unauthorized changes to the bidding documents, which could potentially indicate collusion between the Procurement Service Unit (ULP) Working Group and e-tender participants.

The MD5summer application is an application used to generate and verify MD5 file checksums, primarily to ensure the digital integrity and authenticity of files. The application generates an MD5 hash value, which serves as a digital fingerprint for each file, and verifies whether the file has been tampered with, corrupted, or modified by comparing the checksum with previously generated values. MD5summer supports batch processing, making it possible to handle

Figure 4. **MD5summer Application**



multiple files simultaneously in a single directory and simplifying the mass generation and verification of checksums. The application features a simple and user-friendly interface, making it widely used by developers and system administrators to audit files and ensure that downloaded or transferred data remains intact and unchanged. Although MD5summer uses the MD5 algorithm, which is now considered less secure for high-level cryptographic purposes, it remains a valuable tool for basic file verification and effectively helps maintain the transparency and integrity of digital data.

Examination of Document Metadata to Assess Authenticity and Consistency

File metadata and properties are examined to verify document authenticity and consistency. Key attributes analyzed include file name, size, format, compression structure, checksum values, and authoring information. Similarities across multiple bidders such as identical file structures, metadata, and checksums are treated as indicators of potential coordinated document preparation or manipulation.

To trace the digital footprint of documents, including upload history, modifications, and user access, auditors compare the file properties or metadata with data recorded in the system to ensure that the document truly originates from the participant and is not manipulated during the procurement process. This comparison serves as a verification step to confirm the document's authenticity and integrity, ensure compliance with applicable procurement standards, and identify potential unauthorized changes or tampering. Testing of metadata or properties of the price bidding document file is the process of examining and verifying the technical attributes and properties of files uploaded by tender participants in order to ensure the authenticity, consistency and integrity of the submitted bidding documents.

From the data provided for the price bidding files from three participants, CV. AT, CV. BK, and CV. RAG, the following can be analyzed:

a. Similarity in Name and File Format
   All three files have similar or identical names, such as LIST OF QUANTITIES. xlsx or variations thereof, and are all in .xlsx (Microsoft Excel) format. This indicates that all three participants use the same document type in a standard submission format.
b. File Size and Type
   All three files are the same size, about 848 kB, and are of the MIME type corresponding to an Excel document (application/vnd.openxmlformats-officedocument.spreadsheetml.sheet).
c. ZIP Properties and Compression
   The .xlsx files are actually compressed ZIP files. All three files use the deflated compression method with the same zip_bit_flag and zip_required_version parameters and have a deflated modification date (1980:01:01), indicating the same file structure.

d. CRC Checksum and Compression Size
   All three files have the same CRC (checksum) value of "0x5fc1eb32," and the same compressed and uncompressed file sizes of "30746" and "1108," respectively. This reinforces the indication that the file contents are identical.
e. Document Metadata
   a) Creator and Last Modified By: All three files are created and last modified by "Asus".
   b) The application information used in all three files is Microsoft Excel version 16.03.
   c) The document has 1 worksheet with several named ranges and the same print areas, indicating similar document structure content.

Identification of Collusion Patterns through IP Address Analysis

IP address analysis is conducted to identify patterns of shared or identical access among different bidders. The use of the same IP address across multiple participants is considered a red flag indicating possible collusion or centralized control of bidding activities. Network patterns are mapped to assess relationships and potential coordination among bidders.

The auditors find that several bidders use the same IP address when accessing the LPSE system, indicating potential collusion or unfair cooperation. This finding raises concerns about the integrity of the bidding process, as the use of a shared IP address can indicate that bidders are not acting independently, violating the principles of fairness and transparency in procurement. The auditors will conduct further investigation to determine the extent of the collaboration and assess its impact on the integrity of the e-tender process.

"The auditors analyze the similarity of IP addresses used by participants from the registration stage to the submission of objections. Identification of similar IP addresses raises concerns that one party may have used multiple user IDs to manipulate auction results and gain an unfair advantage in winning certain tender packages. This potential manipulation can undermine the principles of fairness and transparency in the procurement process. Therefore, the auditors will conduct further investigations to determine any indications of collusion or violations of applicable procurement regulations."

Figure 5 shows indications of unauthorized collaboration (collusion) between tender participants in the e-tender process (relationship based on similarity of IP Address carried out by CV. AT as the tender winner, CV. RAG, and CV. BK) based on the similarity or sameness of IP address when uploading the tender documents with the following explanation:

a. Parties Involved:
   a) CV. AT (green): Appointed as the tender winner.
   b) CV. BK (red): One of the tender participants marked with potential irregularities.
   c) CV. RAG (yellow): Identified as a tender participant potentially affiliated with other bidders.
b. Identical IP Address:
   a) The three participants were found to be accessing the e-procurement system using the same IP address, 36.82.99.234. This raises concerns about potential coordination or collusion among the bidders, as the use of a shared IP address could indicate that one party controls multiple user accounts in the e-tender process.
   b) CV. AT and CV. BK also used the same IP address, 36.82.99.245, when participating in the e-procurement process.
   c) CV. RAG was recorded as accessing the e-procurement system via IP address 36.82.99.234.
c. Relationship Flow (Marked with Numbers):
   a) 1.a & 1.b: CV. AT, CV. RAG, and CV. BK used the same IP address (36.82.99.234) when uploading their tender documents. This indicates a potential relationship or coordinated

activity between the two entities.

b) 2: CV. AT and CV. BK were also found to be using the same IP address (36.82.99.245), suggesting a possible relationship between the two.

Assessment of System Availability to Detect Potential Manipulation of Access During Critical Bidding Periods

System access logs and server performance data are analyzed to evaluate the availability of the LPSE application during critical submission periods. This procedure aims to detect abnormal access restrictions or system disruptions that may disadvantage certain participants and indicate intentional manipulation of system availability.

Several providers report challenges uploading bid documents due to network capacity issues during the crucial period leading up to the bid submission deadline. Auditors suspect that these challenges are not solely due to technical issues but may indicate a systematic effort to restrict access after certain bids are accepted. This suspicion raises concerns about the potential for deliberate manipulation of the system to favor certain bidders by preventing their competitors from submitting bids on time.

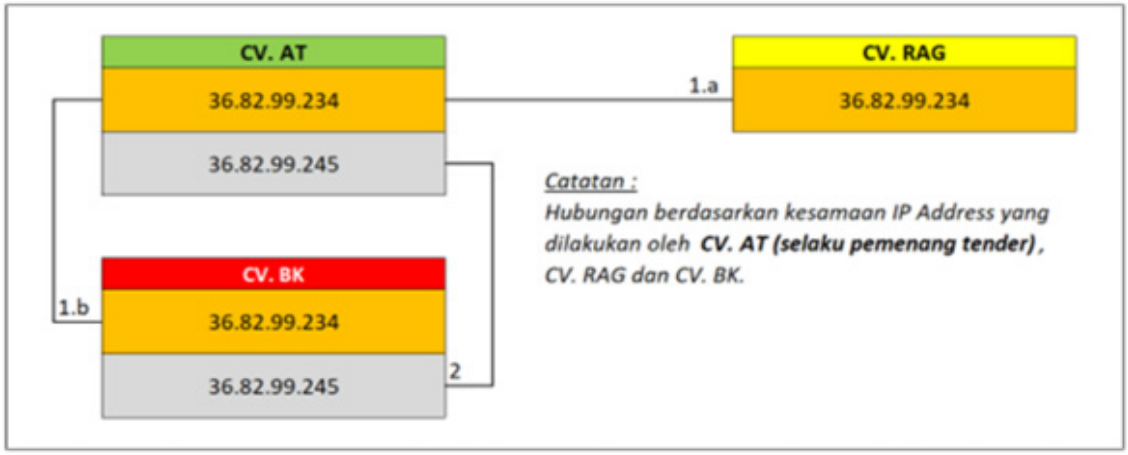
To ensure transparency and fairness in the tender process, auditors analyze system access logs and server availability patterns throughout the tender period. The audits are conducted to detect potential deliberate access manipulation and to ensure that all participants have equal access and use of the e-procurement (LPSE) application throughout the procurement process.

If necessary, the auditor can recommend a forensic audit of the e-procurement (LPSE) server to analyze activity during the e-tender period. This audit aims to uncover indications of deliberate access manipulation to benefit certain parties by examining server logs and system configurations.

All analyses are conducted using a forensic and evidence-based approach, emphasizing data integrity, validity, and traceability. Cross-validation techniques such as log correlation, metadata comparison, and hash verification are employed to ensure the reliability of findings. The audit procedure for selecting providers through the e-procurement (LPSE) has identified vulnerabilities in the e-tender system, particularly in terms of security and integrity, including data manipulation practices, access violations, and indications of collusion between participants.

The findings indicate that, despite the existence of a comprehensive regulatory framework governing e-procurement and e-audit in Indonesia, significant gaps remain between formal compliance and actual implementation practices. Empirical evidence reveals recurring anomalies, including unauthorized use of user IDs, inconsistencies in access logs, identical

Figure 5. **Flow of Potential Collusion or Illegal Cooperation between E-Tender Participants**



document structures, and similarities in IP addresses among bidders. These patterns suggest not only weaknesses in internal control mechanisms but also potential fraud risks, such as collusion and unauthorized system access, which undermine the principles of transparency and fair competition mandated by procurement regulations.

From a governance perspective, the persistence of conventional, non-integrated audit practices limits the effectiveness of oversight in digital environments. The current e-audit approach, which primarily emphasizes data access rather than analytical integration within the LPSE system, creates opportunities for manipulation that may not be readily detected through standard procedures. This finding highlights a critical gap between regulatory intent and operational capability, particularly in addressing technologically enabled fraud schemes.

Therefore, strengthening e-audit requires a shift toward a more integrated, data-driven, and forensic-oriented approach. Embedding analytical procedures such as log correlation, metadata validation, and pattern recognition within the e-procurement system is essential to enhance real-time monitoring and early detection of irregularities. Such improvements are crucial to ensuring the integrity, accountability, and reliability of electronic procurement systems in line with good governance principles.

4. RESULTS AND DISCUSSION

This study identified multiple vulnerabilities in the e-procurement (LPSE) system, including data manipulation, unauthorized access, and indications of collusion among participants. The findings reveal the use of unauthorized user IDs, inconsistencies in activity logs, weak access control mechanisms, similarities in IP addresses, and identical document metadata among bidders (ACFE, 2022; COSO, 2013).

The presence of identical document structures, hash values, and metadata indicates a high likelihood of coordinated behavior among participants, which violates the principles of fair competition in procurement (OECD, 2016). In addition, similarities in IP addresses among bidders strengthen the indication of collusion or bid rigging practices (Liu et al., 2020). These findings demonstrate that despite the existence of regulatory frameworks governing e-procurement, the LPSE system remains vulnerable to fraud risks that threaten transparency, accountability, and fairness in public procurement processes.

Discussion

The findings indicate a gap between regulatory compliance and practical implementation within the LPSE system. From an internal control perspective, these weaknesses reflect deficiencies in control activities, monitoring, and system integration (COSO, 2013). This condition aligns with the concept that ineffective controls increase the likelihood of fraud occurrence (Arens et al., 2020).

From a fraud theory perspective, the identified vulnerabilities can be explained using the fraud framework, where opportunity arises due to weak controls and limited monitoring (ACFE, 2022; Klitgaard, 1998). These conditions enable unauthorized access, data manipulation, and collusive practices in the procurement process.

The findings also support prior studies emphasizing the importance of digital forensic techniques in fraud detection. The use of metadata analysis, hash verification, and log analysis enhances the reliability of audit evidence and supports fraud identification (Singleton & Singleton, 2010; Zhang & Zhao, 2021).

To address these issues, strengthening cybersecurity and access control mechanisms is essential, particularly through multi-factor authentication and role-based access systems (Behl & Behl, 2017). In addition, integrating automated and data-driven audit systems can improve monitoring effectiveness and anomaly detection (Vasarhelyi et al., 2015).

Furthermore, improving auditor competence in digital forensics and IT-based auditing is crucial to enhance audit quality and effectiveness (BPKP, 2021). These improvements are necessary to align e-audit practices with good governance principles and to reduce corruption risks in public procurement (KNKG, 2006; OECD, 2016).

5. CONCLUSION

This study concludes that the implementation of e-audit in the e-procurement (LPSE) system has not been fully effective in mitigating fraud risks. Although regulatory frameworks are in place, significant gaps remain in system integration, access control, and analytical capabilities. The findings reveal vulnerabilities such as unauthorized access, data inconsistencies, and indications of collusion, which highlight the limitations of current audit practices that remain partially manual and lack real-time analytical integration.

Strengthening e-audit requires a technology-driven approach, including enhanced system security, automated audit tools, and periodic forensic evaluations. Improving auditor competence is also essential to support more effective oversight. Overall, strengthening e-audit practices is critical to ensuring transparency, accountability, and integrity in electronic procurement systems, as well as reducing corruption risks in public sector governance.

REFERENCES

Arens, A. A., Elder, R. J., & Beasley, M. S. (2020). *Auditing and Assurance Services: An Integrated Approach* (17th ed.). Pearson.

Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations: Global Study on Occupational Fraud and Abuse*. ACFE.

Badan Pengawasan Keuangan dan Pembangunan (BPKP). (2021). *Pedoman Audit Berbasis Teknologi Informasi*. BPKP.

Behl, A., & Behl, K. (2017). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control Integrated Framework*. COSO.

Hunton, J. E., Wright, A. M., & Wright, S. (2004). Are Financial Auditors Overconfident in their Ability to Assess Risks Associated with Enterprise Resource Planning Systems?. *Journal of Information Systems*, *18*(2), 7–28.

Kementerian Keuangan Republik Indonesia. (2020). *Standar Audit Intern Pemerintah Indonesia (SAIPI)*. Kementerian Keuangan Republik Indonesia.

Klitgaard, R. (1998). *Controlling Corruption*. University of California Press.

KNKG. (2006). *Pedoman Umum Good Corporate Governance Indonesia*. Komite Nasional Kebijakan Governance.

Lembaga Kebijakan Pengadaan Barang/ Jasa Pemerintah (LKPP). (2022). *Peraturan LKPP tentang Sistem Pengadaan Secara Elektronik (SPSE)*. LKPP.

Liu, Q., Luo, X., & Wang, S. (2020). Detecting Collusion in Procurement Auctions: Evidence from E-Procurement Systems. *Electronic Commerce Research*, *20*(3), 567–589.

OECD. (2016). *Preventing Corruption in Public Procurement*. OECD Publishing.

Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting* (4th ed.). John Wiley & Sons.

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in Accounting: An Overview. *Accounting Horizons*, *29*(2), 381–396.

Zhang, J., & Zhao, Y. (2021). Digital Forensic Analysis in E-Procurement Systems: A Framework for Fraud Detection. *Journal of Digital Forensics, Security and Law*, *16*(1), 45–60.

Appendix 1. **Testing Metadata or Properties of the Price Bidding Document File**

1159026106 CV. AT	1158995106 CV. BK	1159092106 CV. RAG
1	2	3
file_name	file_name	file_name
LIST OF QUANTITIES.xlsx	LIST OF QUANTITIES.xlsx	LIST OF QUANTITIES.xlsx
file_size	file_size	file_size
848 kB	848 kB	848 kB
file_type	file_type	file_type
XLSX	XLSX	XLSX
file_type_extension	file_type_extension	file_type_extension
Xlsx	Xlsx	Xlsx
mime_type	mime_type	mime_type
application/vnd. openxmlformats-officedocument. spreadsheetml.sheet	application/vnd. openxmlformats-officedocument. spreadsheetml.sheet	application/vnd. openxmlformats-officedocument. spreadsheetml.sheet
zip_required_version	zip_required_version	zip_required_version
20	20	20
zip_bit_flag	zip_bit_flag	zip_bit_flag
0x0006	0x0006	0x0006
zip_compression	zip_compression	zip_compression
Deflated	Deflated	Deflated
zip_modify_date	zip_modify_date	zip_modify_date
1980:01:01 00:00:00	1980:01:01 00:00:00	1980:01:01 00:00:00
zip_crc	zip_crc	zip_crc
0x5fc1eb32	0x5fc1eb32	0x5fc1eb32
zip_compressed_size	zip_compressed_size	zip_compressed_size
1108	1108	1108
zip_uncompressed_size	zip_uncompressed_size	zip_uncompressed_size
30746	30746	30746
zip_file_name	zip_file_name	zip_file_name
[Content_Types].xml	[Content_Types].xml	[Content_Types].xml
preview_wmf	preview_wmf	preview_wmf
(Binary data 55046 bytes)	(Binary data 51394 bytes)	(Binary data 54862 bytes)
Creator	Creator	creator
Asus	Asus	Asus
last_modified_by	last_modified_by	last_modified_by
Asus	Asus	Asus
create_date	create_date	create_date
2023:05:10 17:55:46Z	2023:05:10 16:42:39Z	2023:05:11 16:08:08Z
modify_date	modify_date	modify_date
2023:05:10 17:57:03Z	2023:05:10 16:44:51Z	2023:05:11 16:09:04Z
Application	Application	application

1159026106 CV. AT	1158995106 CV. BK	1159092106 CV. RAG
1	2	3
Microsoft Excel	Microsoft Excel	Microsoft Excel
doc_security	doc_security	doc_security
None	None	None
scale_crop	scale_crop	scale_crop
No	No	No
HeadingPairs	HeadingPairs	HeadingPairs
0	0	0
Worksheets	Worksheets	Worksheets
1	1	1
4	4	4
2	2	2
Named Ranges	Named Ranges	Named Ranges
3	3	3
4	4	4
links_up_to_date	links_up_to_date	links_up_to_date
No	No	No
shared_doc	shared_doc	shared_doc
No	No	No
hyperlinks_changed	hyperlinks_changed	hyperlinks_changed
No	No	No
app_version	app_version	app_version
16,03	16,03	16,03
Category	Category	category
Application	Application	application
raw_header	raw_header	raw_header
50 4B 03 04 14 00 06 00 08 00 00 00 21 00 32 EB C1 5F 54 04 00 00 1A 78 00 00 13 00 08 02 5B 43 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	50 4B 03 04 14 00 06 00 08 00 00 00 21 00 32 EB C1 5F 54 04 00 00 1A 78 00 00 13 00 08 02 5B 43 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	50 4B 03 04 14 00 06 00 08 00 00 00 21 00 32 EB C1 5F 54 04 00 00 1A 78 00 00 13 00 08 02 5B 43 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
REKAP!Print_Area	REKAP!Print_Area	REKAP!Print_Area
Company	Company	company
TitlesOfParts	TitlesOfParts	TitlesOfParts
0	0	0
REKAP	REKAP	REKAP
1	1	1
DKH	DKH	DKH

1159026106 CV. AT	1158995106 CV. BK	1159092106 CV. RAG
1	2	3
raw_header	raw_header	raw_header
2	2	2
DKH (2)	DKH (2)	DKH (2)
3	3	3
DKH (3)	DKH (3)	DKH (3)
4	4	4
DKH!Print_Area	DKH!Print_Area	DKH!Print_Area
5	5	5
'DKH (2)'!Print_Area	'DKH (2)'!Print_Area	'DKH (2)'!Print_Area
6	6	6
'DKH (3)'!Print_Area	'DKH (3)'!Print_Area	'DKH (3)'!Print_Area
7	7	7

Source: Processed Data